

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

---

1. (Currently Amended) A security system for a computer connected to a network of computers comprising:

at least one security subsystem associated with said computer, said subsystem being configured to ~~automatically and without human control correlate~~ monitor and analyze for security events across a plurality of devices associated with said network of computers, ~~and to detect attacks on said computer~~ and to respond to said detected attacks;

a master system;

E and a secure link between said security subsystem and a said master system enabling data communication therebetween;

wherein said security subsystem responds to said detected attacks by selectively reporting a status of said network of computers to said master system, testing said network of computers and implementing countermeasures; and wherein said master system automatically and without human control monitors analyzes said security subsystem through said secure link by at least testing said security subsystem, allows said subsystem to respond to said detected attacks by selectively reporting, testing and implementing countermeasures, and registers information pertaining to attacks detected by said security subsystem.

2. (Original) The security system of Claim 1 further comprising a pseudo attack generator associated with said master system for generating attacks on said computer detectable

by said security subsystem wherein said master system monitors said security subsystem by comparing said pseudo-attacks to said attacks detected by the security subsystem.

3. (Original) The security system of Claim 1 wherein said master system is hierarchically independent from said security subsystem.

4. (Original) The security system of Claim 1 wherein said security subsystem is hierarchically subordinate to said master system.

5. (Currently Amended) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network, said subsystem being configured to ~~automatically and without human control~~ correlate monitor and analyze for security events across a plurality of devices associated with said target network of computers, ~~and to detect attacks on said network~~ and to respond to said detected attacks;

a master system;

and a secure link between said security subsystem and a said master system enabling data communication therebetween;

wherein said security subsystem responds to said detected attacks by selectively reporting a status of said target network to said master system, testing said target network and implementing countermeasures; and wherein said master system ~~automatically and without human control monitors~~ analyzes said security subsystem through said secure link by at least testing said security subsystem, allows said subsystem to respond to said detected attacks by

selectively reporting, testing and implementing countermeasures, and registers information pertaining to the attacks detected by said security subsystem.

6. (Original) The network security system of Claim 5 wherein said master system is hierarchically independent from said security subsystem.

7. (Original) The network security system of Claim 5 wherein said security subsystem is hierarchically subordinate to said master system.

8. (Currently Amended) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network and configured to ~~automatically and without human control correlate~~ monitor and analyze for security events across a plurality of devices associated with said target network, ~~and~~ to detect and register attacks on said target network and to respond to said detected attacks;

a master system

a secure link for data communication between said security subsystem and said master system; and

testing means associated with said master system for generating pseudo-attacks on said target network initiated by said master system and detectable by said security subsystem;

wherein said security subsystem responds to said detected attacks by selectively reporting a status of said target network to said master system, testing said target network and implementing countermeasures; and wherein said master system ~~automatically and without human~~

~~control monitors~~ analyzes said security subsystem through said secure link by at least testing said security subsystem and comparing the pseudo-attacks generated by said testing means to the detected attacks registered by said security subsystem, and allows said subsystem to respond to said detected attacks by selectively reporting, testing and implementing countermeasures.

9. (Original) The network security system of Claim 8 wherein said master system is hierarchically independent from said security subsystem.

10. (Original) The network security system of Claim 8 wherein said security subsystem is hierarchically subordinate to said master system.

11. (Currently Amended) A method for monitoring the integrity of a security subsystem associated with a target network of computers and configured to detect attacks on said network of computers comprising:

~~automatically and without human control correlating~~ monitoring and analyzing for security events across a plurality of devices associated with said target network, detecting and registering attacks on said target network using said security subsystem;

responding to said detected attacks by selectively reporting a status of said target network from said security subsystem to said master system, testing said target network using said security subsystem and implementing countermeasures by said security subsystem;

establishing a secure link for the transfer of data between said security subsystem and a master system hierarchically independent from said security subsystem;

~~automatically and without human control monitoring~~ analyzing the status of said security subsystem through said secure link by at least testing said security subsystem; and registering information pertaining to the status of said security subsystem.

12. (Original) The method for monitoring the integrity of a security system of Claim 11 including the steps of:

connecting said master system and said target network separately to an open network of computers;

generating at least one pseudo-attack in said master system, said pseudo attack being detectable by said security subsystem;

generating in said master system a list of expected responses to said at least one pseudo-attack;

delivering said at least one pseudo-attack over said open network to said target network; and

comparing the response of said security subsystem to said pseudo-attack to the list of expected responses thereto.

13. (Currently Amended) A security system for a computer connected to a computer network comprising:

at least one detection means associated with said computer, said detection means being configured to ~~automatically and without human control correlate~~ monitor and analyze for security events across a plurality of devices associated with said computer network, ~~and~~ to detect an attack on said computer and to respond to said detected attacks;

a master security system located outside said computer network; and

a secure link between said detection means and said master security system enabling data communication therebetween;

wherein said detection means responds to said detected attacks by selectively reporting a status of said network of computers to said master system, testing said network of computers and implementing countermeasures; and wherein said master security system automatically and without human control monitors analyzes said detection means through said secure link by at least testing said detection means, allows said detection means to respond to said detected attacks by selectively reporting, testing and implementing countermeasures, and registers information pertaining to attacks detected by said detection means.

E/ 14. (Original) The security system of Claim 13, wherein said detection means is one or more selected from the group consisting of an intrusion detection system, a firewall and a security subsystem.

15. (Original) The security system of Claim 13, wherein said master security system is hierarchically independent from said detection means.

16. (Original) The security system of Claim 13 further comprising a pseudo attack generator associated with said master security system for generating attacks on said computer detectable by said detection means wherein said master security system monitors said detection means by comparing said pseudo-attacks to said attacks detected by said detection means.

17. (Currently Amended) A network security system for a target network of computers comprising:

at least one detection means associated with said target network, said detection means being configured to ~~automatically and without human control correlate~~ monitor and analyze for security events across a plurality of devices associated with said computer network, ~~and to detect an attack on said network~~ and to respond to said detected attacks;

a master security system located outside said network; and

a secure link between said detection means and said master security system enabling data communication therebetween;

wherein said detection means responds to said detected attacks by selectively reporting a status of said target network to said master system, testing said target network and implementing countermeasures; and wherein said master security system analyzes ~~automatically and without human control monitors~~ said detection means through said secure link by at least testing said detection means, allows said detection means to respond to said detected attacks by selectively reporting, testing and implementing countermeasures, and registers information pertaining to attacks detected by said detection means.

18. (Original) The network security system of Claim 17, wherein said detection means is one or more selected from the group consisting of an intrusion detection system, a firewall and a security subsystem.

19. (Original) The network security system of Claim 17, wherein said master security system is hierarchically independent from said detection means.

20. (Original) The network security system of Claim 17 further comprising a pseudo-attack generator associated with said master security system for generating attacks on said target network detectable by said detection means wherein said master security system monitors said detection means by comparing said pseudo-attacks to said attacks detected by said detection means.

21. (Currently Amended) A method for monitoring the integrity of a detection means associated with a computer, said computer being connected to a computer network, and configured to detect an attack on said computer, said method comprising the steps of:

E1  
~~automatically and without human control correlating~~ monitoring and analyzing  
for security events across a plurality of devices associated with said computer network, detecting  
and registering attacks on said computer network using said detection means;

responding to said detected attacks by selectively reporting a status of said  
computer network from said detection means to said master system, testing said computer  
network using said detection means and implementing countermeasures by said detection means;

establishing a secure link for the transfer of data between said detection means  
and a master system hierarchically independent from said detection means;

~~automatically and without human control monitoring~~ analyzing the status of said  
detection means through said secure link by at least testing said detection means; and

registering information pertaining to the status of said detection means.

22. (Currently Amended) A method for monitoring the integrity of a detection means associated with a target network of computers and configured to detect an attack on said network of computers comprising the steps of:

~~automatically and without human control correlating~~ monitoring and analyzing for security events across a plurality of devices associated with said target network, detecting and registering attacks on said target network using said detection means;

responding to said detected attacks by selectively reporting a status of said target network from said detection means to said master system, testing said target network using said detection means and implementing countermeasures by said detection means;

establishing a secure link for the transfer of data between said detection means and a master system hierarchically independent from said detection means;

~~automatically and without human control monitoring~~ analyzing the status of said detection means through said secure link by at least testing said detection means; and

registering information pertaining to the status of said detection means.